THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MARYLAND

GREENBELT DIVISION

ANNA L. HALEY, an Individual, on behalf of herself and all others similarly situated, Plaintiff, vs. MARRIOTT INTERNATIONAL, INC., 10400 Fernwood Road Bethesda, Maryland 20817 (a Montgomery County, Maryland Resident) Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Anna L. Haley, individually and on behalf of all others similarly situated, by and through her undersigned counsel, for her complaint brings this class action for damages and equitable relief against Defendant Marriott International, Inc. Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge:

PRELIMINARY STATEMENT

1. This is a civil action brought by Plaintiff Anna L. Haley ("Haley" or "Plaintiff") on behalf of herself and all others similarly situated against Defendant Marriott International, Inc. ("Marriott" or "Defendant"). In this action, Plaintiff alleges that Marriott allowed a massive data breach in which the sensitive personal information of Plaintiff and millions of other consumers was stolen by unknown persons (the "Data Breach").

2. With headquarters in Bethesda, Maryland, in the Washington, D.C. metropolitan area, Marriott is the world's largest hotel chain, with over 30 hotel brands, comprising more than 6,500 properties and 1.2 million rooms in more than 127 countries and territories. Many of its hotel brands were acquired by Marriott in a 2016 merger with Starwood Hotels and Resorts Worldwide, LLC.

3. Marriott maintains the Starwood Preferred Guest program and Starwood guest reservation database, acquired in the 2016 merger. Members and guests who stay at Marriott's Starwood hotels have their personal information entered into the Starwood guest reservation database. Since 2014, some 500 million guests have made reservations at Marriott's Starwood properties.

4. On November 30, 2018, Marriott disclosed that an unauthorized third party has, since 2014, been accessing the Starwood guest reservation database ("Starwood Database"), acquiring the personal information of some 500 million consumers, including names, addresses, telephone numbers, and other sensitive and confidential personal and financial information (the "Personal Information").

5. Marriott failed to take the measures that it knew were necessary to protect the sensitive data in its keeping, and the direct result is the largest consumer data breach of its kind in history. Because of Defendant's negligence, the Personal Information of Plaintiff and many millions of other of Defendant's guests is now in the hands of unknown hackers and may be used for identity theft and other injurious purposes.

6. Plaintiff is a member of the Starwood Preferred Guest program who has made reservations through the Starwood system and stayed as a guest in Defendant's Starwood hotels during the relevant time period, and whose Personal Information, upon information and belief,

has been stolen in the Data Breach.

7. Plaintiff reasonably relied on Marriott to keep her Personal Information safe from hackers, and would not have entrusted her private data to Defendant had she known that it would not take those measures necessary to protect her Personal Information from data thieves.

8. Accordingly, Plaintiff brings this case as a class action and, on behalf of herself and other similarly situated persons, seeks damages including compensatory damages, statutory and punitive damages, as well as injunctive and equitable relief, declaratory relief, and attorney fees and costs.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interests and costs; the number of Class members exceeds 100; and Plaintiff and many members of the proposed Class are citizens of different states than the Defendant.

10. This Court has personal jurisdiction over the Defendant because it maintains its principal place of business and its corporate headquarters in this State and District, and as it conducts substantial business in this State and Judicial District.

11. Venue is proper in this Judicial District because the Defendant conducts substantial business in this Judicial District, Defendant is a resident of the Judicial District, and/or the conduct complained of occurred in or emanated from this District.

PARTIES

12. Plaintiff Anna L. Haley is a citizen and resident of California. She is and at all relevant times has been a participant in the Starwood Preferred Guest Program. During the relevant period, Haley has used the Starwood system to make reservations and has stayed as a hotel guest in Starwood properties.

13. Ms. Haley's Personal Information was stored by Marriott in the Starwood Database, and was stolen by unknown hackers in the Data Breach complained of herein.

14. Defendant Marriott International, Inc., a Montgomery County, Maryland resident, is the world's largest hotel chain. Marriott is a Delaware corporation with its headquarters and principal place of business at 10400 Fernwood Road, Bethesda, Maryland 20817.

15. For the fiscal year 2017, Marriott reported revenues of US $22.894 billion. Marriott is a publicly-traded company, with a market capitalization of US $39.1 billion as of October 2018.

FACTUAL BACKGROUND

With the Acquisition of Starwood, Marriott is the World's Largest Hotel Chain

16. Marriott is an American multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities.

17. On September 23, 2016, Marriott acquired Starwood Hotels and Resorts Worldwide, LLC ("Starwood"), becoming the largest hotel chain in the world. Marriott's Starwood brands include W hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton and Design Hotels, and timeshare properties Sheraton

Vacation Club, Westin Vacation Club, The Luxury Collection Residence Club, St. Regis Residence Club and Vistana.

18. The Starwood purchase gave Marriott more leverage with corporate travel departments, and with online travel agencies such as Expedia and Priceline.

19. Marriott has more than 6,500 properties in 127 countries and territories globally, giving it more than 1.2 million hotel rooms, with an additional 195,000 rooms in the development pipeline.

20. Like other hotel chains, Marriott owns very few individual hotels. Instead, it franchises its branded hotels to hundreds of individual owners, generally real estate development companies. Marriott handles promotion and marketing for its chain, and maintains loyalty programs and clubs such as the Starwood Preferred Guest program, which promises consumers points and other benefits for membership.

21. Following its 2016 acquisition of Starwood, Marriot owns and controls the Starwood guest reservation system and database at issue here.

The Breach of the Starwood Guest Reservation Database Has Exposed the Personal Information of Plaintiff and As Many as 500 Million Class Members

22. Marriott maintains the Starwood Preferred Guest program and the Starwood guest reservation database ("Starwood Database"). Contained in the Starwood Database is the Personal Information of some 500 million consumers, including that of Plaintiff, other members of the Starwood Preferred Guest program and other guests who have made reservations to stay at Marriott's Starwood properties.

23. On November 30, 2018, Marriott publicly announced that it had discovered a massive breach of the Starwood Database (the "Data Breach").[1] Marriott stated that on September 8, 2018, it had received an alert from an internal security tool regarding an attempt to access the Starwood Database. Marriott stated that upon investigation, it discovered that an unauthorized party had been accessing the Starwood Database since 2014, copying the Personal Information of guests.

24. According to Marriott, the stolen data includes the Personal Information of up to 500 million guests who made a hotel reservation at a Starwood property between 2014 and September 10, 2018. For approximately 327 million of these Starwood guests, the stolen Personal Information includes some combination of the guest's name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

25. For some guests, the stolen Personal Information also includes credit/payment card numbers and expiration dates. Marriott states payment card numbers were stored in the Starwood Database in encrypted form using AES-128 encryption. However, Marriott states that it does not know whether the two components needed to decrypt the payment card numbers were also taken in the data breach.

26. The Data Breach occurred because Marriott failed to implement and maintain protocols and measures customary in the industry to protect its guests' private information in the Starwood guest reservation database. Plaintiff and Class members never would have entrusted

[1] *See Marriott Announces Starwood Guest Reservation Database Security Incident*, found at http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last visited Dec. 9, 2018).

their Personal Information to Defendant had they known it would not take adequate measures to protect their data.

27. Marriott still has still not disclosed the full extent and scope of the Data Breach.

The Stolen Personal Informal of Plaintiff and Class Members Can Now Be Used for Identity Theft and Other Injurious and Fraudulent Purposes

28. Theft of personal information is a serious and growing problem in the United States. According to Javelin Strategy & Research, the overall identity fraud incidence rose 16% in 2016 to affect 6.15% of U.S. consumers—with 15.4 million U.S. identity theft victims, who lost a total of $16 billion.

29. As tracked by the Consumer Sentinel Network, maintained by the Federal Trade Commission, of the 3.1 million consumer fraud complaints filed with law enforcement and private agencies in 2015, 16 percent related to identity theft, with identity theft complaints increasing by more than 47 per cent from 2014.

30. New account fraud, one of the more injurious forms of identity theft, more than doubled (up 113%) between 2014 and 2015.[2]

31. The theft of Personal Information is what makes identity theft possible.[3] Stolen Personal Information can be used for many nefarious purposes injurious to the rightful owners of the information, including: opening credit card accounts or taking out loans in the victims' names, changing billing addresses to conceal bill statements, obtaining mobile phones, opening

---

[2] *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?,* found at https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited Dec. 9, 2018).

[3] *Id.*

bank accounts and writing bad checks, withdrawing victims' funds using their debit card numbers, and using victims' identities in the event of an arrest or court action.[4]

> Consider this scenario, familiar to many Americans: you're at work and expecting a call from a handyman about the appointment the next day. You don't recognize the number when your phone rings, but you answer, thinking it must be the handyman. Instead, it's a bill collector asking you to make a payment on a loan. The bill collector has your name, phone number, address and even knows your social security number.
>
> The problem is that you didn't take out the loan. This likely means that someone else applied for and secured the loan using your Personal Information, such as your name, address and social security number. This is called new account fraud, and the Javelin report referenced above found that new account fraud more than doubled (up 113%) from 2014 to 2015. They called it "the most expensive and highest-impact" fraud for consumers.[5]

32. Stolen Personal Information is often offered for sale on the "dark web," the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.[6] On the dark web, blocks of stolen identity information are traded or sold to anonymous buyers. Often the transactions are in bitcoin or utilize other untraceable methods of payment. Once purchased on the dark web, the buyer can use the personal data to gain access to different areas of the victim's digital life, including social media and email accounts. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends and colleagues.

33. Recently, investigators discovered the Data Breach may have ties to intelligence-gathering efforts by China's Ministry of State Security, China's Communist-controlled civilian

---

[4] *Id.*

[5] *Id.*

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* found at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 11, 2018).

spy agency. If true, the victims' safety is at risk, especially given that Marriott is the top hotel provider for American government and military personnel.[7]

Marriott's Inadequate Remedial Efforts, and the Continuing Harm Caused Plaintiff and Other Victims of the Data Breach

34. According to a study by Javelin Strategy & Research, there is a high correlation between having information taken in a data breach and becoming an identity theft victim, with nearly 1 in 4 data breach notice recipients becoming an actual victim of identity fraud. The danger of stolen Personal Information being used for identity theft and other fraud also persists for years after the theft. Thus, Plaintiff and Class members face years of being at risk for identity theft, with a 1 in 4 chance that they will have their identities fraudulently used.

35. To mitigate the effect of the Data Breach, victims and Class members have several options, none of which are adequate to protect fully against identity theft or other harm. Employing protective measures also will require time, effort, and continued vigilance for years to come. This prolonged effort to trace and mitigate harm caused by the Data Breach will result in additional stress, anxiety, and inconvenience to Plaintiff and Class members.

36. The services offered by Marriott to address the Data Breach are inadequate to protect victims. Marriott has not even provided full information on the extent and scope of the Data Breach. Marriott has established a dedicated call center for potential victims to inquire about the Data Breach, but admits the call center hotlines are impacted and callers may spend extended periods of time to get through to an agent.[8]

37. Marriott has also provided victims the option of enrolling for WebWatcher,

---

[7] See https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html (last visited Dec. 11, 2018)

[8] https://answers.kroll.com/ (last visited Dec. 11, 2018).

a service that monitors internet sites where stolen Personal Information is shared and that will generate an alert if the consumer's Personal Information is found, free for one year.[9] But, evidence of identity theft may take longer than one year to surface, and subscribers will therefore need to pay $160 to continue the service after the first year and for years thereafter.[10]

38. One option for victims is instituting a "credit freeze," also known as a security freeze, which restricts access to the consumers' credit reports. Because most creditors need to view credit reports prior to opening new accounts, a credit freeze may make it harder for cybercriminals to apply for loans and credit cards, or open accounts using stolen information.[11] But, a credit freeze may not be an effective obstacle, as there are multiple uses for stolen Personal Information apart from simply opening credit accounts. Also, buyers of stolen Personal Information can wait months and years before using the data. Thus, a credit freeze may only prevent Plaintiff and Class members from using their own credit, delaying major purchases such as education or a home, and interfering with job opportunities where potential employers check credit reports of job applicants.

39. The stolen Personal Information includes information about travel habits and other private information that may place some victims at risk for blackmail or embarrassment, a danger that none of the available identity-protection measures can address.

40. The stolen passport information is particularly valuable to identity thieves. Like a Social Security number, a passport number is considered by most financial institutions to be

---

[9] *id.*

[10] https://www.webwatcher.com/ (last visited Dec. 11, 2018).

[11] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#what (last visited Dec. 11, 2018).

information that can definitively identify a person, and it can't easily be changed.[12] A new passport presently costs approximately $110 plus the time and effort involved in the process. Though Marriott has offered to pay for replacement passports, it will only do so in instances where it is determined that fraud has already taken place. Because it may be years before a fraud is committed and comes to light, victims are unlikely to benefit from Marriott's promise.[13] Further, if Chinese government-backed hackers conducted the Data Breach for espionage purposes, not identity fraud, no victims will benefit from Marriott's promise.[14] Still, since victims' Personal Information is already exposed, it may very well end up on the dark web eventually.

41. Starwood Preferred Guest members are advised to monitor their SPG accounts because there is a possibility that members' SPG account information will be used to attempt to access and use victims' SPG accounts.[15] SPG account information includes additional personal information of members, including SPG account numbers, loyalty program points balances, status levels, and communication preferences.

42. Marriott further advises victims to engage in other time-consuming

---

[12] *See* https://www.consumerreports.org/data-theft/marriott-data-breach/ (last visited Dec. 9, 2018).

[13] *Marriott Says It Will Pay for Replacement Passports After Data Breach. Here's Why That's Likely Baloney*, found at http://fortune.com/2018/12/08/marriott-breach-hack-starwood-passport-pay/ (last visited Dec. 9, 2018).

[14] See http://fortune.com/2018/12/08/marriott-breach-hack-starwood-passport-pay/ (last visited Dec. 11, 2018)

[15] https://answers.kroll.com/ (last visited Dec. 9, 2018).

activities to determine if their identities have been stolen, including changing their passwords regularly, and reviewing payment card account statements for unauthorized activity.[16] While Class members will be forced to do that and more for years to come, such vigilance does not eliminate the threat, but just increases the burden on victims.

43. As a result of the data breach caused by Marriott's recklessness, Plaintiff's and consumers' Personal Information is now in the hands of unknown hackers, and Plaintiff and the Class now face an imminent, heightened and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendant's conduct. Accordingly, Plaintiff and the Class have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C.Cir. 2017).

CLASS ACTION ALLEGATIONS

44. Plaintiff beings this complaint on behalf of herself and a class ("Class") initially defined as follows:

> **"All persons whose Personal Information was stored in the Starwood guest reservation database at the time of the data breach disclosed by Marriott on November 30, 2018."**

45. Excluded from the Class are Defendant; any parent, affiliate, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any of Defendant's officers or directors; or any successor or assign of Defendant. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

46. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the

[16] *Id.*

putative Class, estimated at 500 million, are so numerous that joinder of all members of any Class would be impracticable. Members of the Class can be readily identified through Defendant's records.

47. **Commonality and Predominance – Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law or fact that exist as to all members of the Class, including, *inter alia*:

a. Whether Defendant failed to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against known and reasonably anticipated threats to security;

b. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

c. Whether Defendant owed a legal duty to Plaintiff and members of the Class to adequately protect their Personal Information;

d. Whether Defendant breached its duty to adequately protect the Personal Information of Plaintiff and members of the Class;

e. Whether Defendant should have known that its Starwood Database was vulnerable to attack and whether it took sufficient steps to prevent such attack;

f. Whether Defendant's actions, or failure to act, was the proximate cause of, or resulted in, the breach of the Starwood Database;

g. Whether Defendant knew about the Data Breach before it was announced to the public and whether Defendant failed to timely notify the public of the Data Breach;

h. Whether Defendant violated the statutes and/or common law referenced herein;

i. Whether Plaintiff and members of the Class suffered legally cognizable damages as a result of Defendant's conduct; and

j. Whether Plaintiff and members of the Class are entitled to injunctive, declarative and/or monetary relief; and the nature of that relief.

48. The questions of law and fact common to the members of the Class predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

49. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members. Plaintiff and all members of the putative Class had Personal Information exposed in the Data Breach, and have been adversely affected and damaged in that Defendant failed to adequately protect the Personal Information in the Starwood Database.

50. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4**). Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members. She has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously.

51. **Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer harm. Even if separate actions could be brought by individual Class members, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, and create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Marriott.

52. **Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).** Marriott has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Federal Rule of Civil Procedure 23(b)(2).

53. **Superiority – Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy. Class action procedures allow a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously providing the unique benefits of unitary adjudication, economies of scale and comprehensive supervision by a single court. By contrast, most Class members lack the financial resources to pursue this matter on an individualized basis and, even if some could afford it, the court system could not. Individualized litigations to resolve a common dispute concerning Marriott's Data Breach would be unduly burdensome to the court system and would result in the duplication of evidence, effort and expense.

FIRST CLAIM FOR RELIEF
NEGLIGENCE
(Brought on Behalf of Plaintiff and the Class)

54. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

55. Defendant owed a duty to Plaintiff and the Class and by its negligence breached that duty.

56. Defendant solicited confidential and sensitive Personal Information from Plaintiff and the Class, and undertook a duty to exercise reasonable care in safeguarding that Personal Information from unauthorized third-party access.

57. Defendant's duty included, *inter alia,* designing, maintaining, and testing its security systems to ensure the Personal Information was secured, encrypted, and protected in compliance with industry customs and practices, and to create and employ processes to timely detect a breach, ascertain the extent of such breach, and to promptly warn Plaintiff and other Class members of that breach.

58. Defendant further had a duty to reasonably destroy Personal Information once it was no longer required, to mitigate the risk of such Personal Information being compromised in a data breach.

59. Defendant's duties arose from its relationship to Plaintiff and Class members and from industry custom and practice.

60. Defendant knew or should have known the sensitive, personal nature of the Personal Information, and the value of the Personal Information to criminals who profit from attaining such information. Defendant, the largest hotel chain in the world, knew or should have known the risks involved in storing the Personal Information and the importance of maintaining secure systems, especially given recent data breaches within the hospitality industry.

61. Defendant knew or should have known its systems did not adequately safeguard Plaintiff and Class members from unauthorized access, usage or disclosure. Defendant's failure to acknowledge and correct ongoing data security problems is evidenced by unauthorized access of the Starwood Database since 2014. Defendant, having acquired Starwood in 2016, had two years to detect the breach and correct its systems, but failed to do so.

62. Defendant knew or should have known Plaintiff and Class members would suffer

additional harm when it failed to warn Plaintiff and Class members of the Data Breach between the time it learned of the unauthorized access on September 8, 2018 and Defendant's public announcement on November 30, 2018, nearly 12 weeks later.

63. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and other Class members, their Personal Information would not have been compromised, accessed, and stolen by unauthorized parties.

64. Now, Plaintiff and other Class members suffer stress and anxiety caused by the knowledge that their Personal Information has been accessed by unknown entities and may be used for nefarious purposes, including credit fraud, identity theft, and espionage. Plaintiff and Class members also suffer consequential costs and inconvenience to procure credit protection services, identity theft insurance, credit freezes, new passports, new debit and credit cards, new telephone numbers, new email addresses, and other protective measures to prevent further harm.

65. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder.

SECOND CLAIM FOR RELIEF
NEGLIGENCE *PER SE*
(Brought on Behalf of Plaintiff and the Class)

66. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

67. The Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 5, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information.

68. Defendant solicited Plaintiff's and other Class members' Personal Information in exchange for Plaintiff's and Class members' ability to obtain Starwood loyalty program points and added convenience and ease when booking reservations at Starwood properties. This Personal Information includes Class members' names and credit card information, which facilitates sales transactions that affect commerce. Plaintiff and Class members entrusted this sensitive data to Defendant with the expectation that Defendant would in turn safeguard the information from unauthorized access and usage.

69. Defendant violated the FTCA by neglecting to implement and maintain adequate security systems to protect Plaintiff's and Class members' Personal Information from the Data Breach. Defendant's failure was not an isolated incident, but a continuous failure to protect Plaintiff's and Class members' Personal Information from the time of Defendant's acquisition of Starwood in 2016. Defendant continued its disregard of Plaintiff's and Class members' privacy and financial safety when it failed to publicly announce the breach between learning of the breach on September 8, 2016 and November 30, 2018. Those nearly 12-weeks could have provided Plaintiff and Class members the opportunity to begin employing tools, such as credit freezes, and adopting measures such changing their card information and informing their financial institutions to mitigate the effects of the Data Breach and prevent further or future harm.

70. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se.*

71. Plaintiff and Class members are within the class of persons that the FTCA was intended to protect.

72. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC actively pursues businesses whose failure to

adhere to the FTCA results in inadequate data security systems and unfair business practices causing similar harm that Plaintiff and Class members now suffer.

73. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer damages arising from the Data Breach. Plaintiff's and Class members' Personal Information has been accessed, requiring Plaintiff and Class members to take disruptive, time consuming, and costly precautions to protect themselves against identity theft. Still, these precautions are no guarantee that Plaintiff's and Class members' Personal Information will not be used in credit fraud or identity theft in the future. Plaintiff and Class members have, through no fault of their own, incurred fees and costs to change their personal financial information, identity documents, and credit cards; freeze or close financial accounts; and procure identity theft protective services.

74. In addition, Plaintiff and Class members must remain vigilant, as they will remain vulnerable to identity theft and fraud for years to come as their Personal Information remains available to unauthorized third parties.

75. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder.

THIRD CLAIM FOR RELIEF
BREACH OF IMPLIED CONTACT
(Brought on Behalf of Plaintiff and the Class)

76. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

77. When Plaintiff and Class members created their Starwood profiles and entered their Personal Information for Defendant, they entered into implied contracts wherein Defendant contracted to use reasonable or industry-standard systems to protect the Personal Information.

78. Defendant benefited from retaining Plaintiff's and Class members' Personal Information. Plaintiff and Class members were more likely to book with Starwood because of the convenience of having personal information automatically entered upon reserving a room and the ability to collect Starwood points toward future stays.

79. In exchange, Defendant implicitly guaranteed, not only to safeguard the Personal Information, but to regularly monitor and test its systems for potential weaknesses, and to notify Plaintiff and Class members in the event of a breach.

80. Plaintiff and Class members would not have provided Defendant with their intimate, sensitive information without Defendant's assurances that the Personal Information was safe in its care.

81. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

82. Defendant breached its implied contracts with Plaintiff and Class members by failing to protect Plaintiff's and Class members' Personal Information, failing to monitor and test its systems for the weaknesses that caused the Data Breach, and failed to timely notify Plaintiff and Class members of the Data Breach.

83. Defendant's breaches of implied contracts with Plaintiff and Class members were the direct and proximate cause of Plaintiff's and Class members' losses and damages sustained herein.

84. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder.

FOURTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(Brought on Behalf of Plaintiff and the Class)

85. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

86. Defendant benefited when Plaintiff and Class members entrusted Defendant with their Personal Information. Among other things, as stated above, Plaintiff and Class members were more likely to create reservations at Starwood properties.

87. Defendant was unjustly enriched by this benefit given that the actions causing Defendant's enrichment caused Plaintiff and Class members harm.

88. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder.

FIFTH CLAIM FOR RELIEF
INVASION OF PRIVACY
(Brought on Behalf of Plaintiff and the Class)

89. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

90. Defendant invaded Plaintiff 's and the Class members' right to privacy when it retained Plaintiff's and the Class members' Personal Information in the Starwood Database and failed to adequately safeguard it from unauthorized access.

91. Given the widespread fear of identity theft and numerous safeguards ordinary persons erect to prevent it, the Data Breach was obviously offensive and objectionable to Plaintiff, Class members, and any reasonable person.

92. Plaintiff and Class members would not have entrusted their most intimate personal and financial data to Defendant without an expectation that Defendant would keep the

data private and secure from unauthorized parties. This entrustment was reasonable as they reasonably believed Marriott would not have become the world largest hotel chain without protecting its guests' privacy.

93. As a proximate result of Defendant's acts and omissions, Plaintiff's and the Class members' Personal Information was compromised, accessed, stolen, and viewed by third parties not authorized by Plaintiff or the Class members, invading their privacy and causing harm.

94. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff 'sand Class members' Personal Information.

95. Unless and until enjoined and restrained by court order, Defendant's wrongful conduct will continue to cause Plaintiff and the Class members great and irreparable injury. Plaintiff's and the Class members' Personal Information continues to be available to be viewed, stolen, distributed and used by unauthorized third parties. Plaintiff and Class members have no adequate remedy at law for their injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class.

96. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder.

SIXTH CLAIM FOR RELIEF
DECLARATORY RELIEF
(Brought on Behalf of Plaintiff and the Class)

97. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

98. Plaintiff and Class members entered into an implied contract wherein they provided Defendant with their Personal Information in exchange for Defendant's assurance that their Personal Information would be kept safe from unauthorized access and usages.

99. Defendant's duty of care arises from this implied contract.

100. Defendant breached this duty when it failed to protect Plaintiff's and Class members' Personal Information and allowed it to be accessed in the Data Breach.

101. Defendant still possesses this Personal Information and has not provided details of any additional safeguards it has now implemented in light of the Data Breach, if any. Defendant has not revealed the full extent of the Data Breach, and there is no reason to believe there are no ongoing or more expansive breaches presently occurring or threatened.

102. In addition, now that Defendant's substandard security measures are public, Plaintiff's and Class members' Personal Information is at even greater risk.

103. Pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq.; Fed. R. Civ. P. 57, Plaintiff and Class members request that the Court enter a judgment declaring, *inter alia*:

a. Defendant owed (and continues to owe) a legal duty to adequately safeguard Plaintiff's and Class members' Personal Information, and timely notify them about any security breach;

b. Defendant breached (and continues to breach) these duties by failing to adequately safeguard Plaintiff's and Class members' Personal Information; and

c. Defendant's breach of its legal duties directly and proximately caused the Data Breach, and the resulting damages, injury and harm suffered by Plaintiff and Class members.

103. Plaintiff and Class members request the Court to enter a judgment pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.;* Fed. R. Civ. P. 57, requiring Defendant to comply with its duty by implementing and maintaining reasonable security measures, including, but not limited to:

a. Creating, implementing and maintaining adequate safeguards to protect against further access to its Starwood Database and any other database containing guests' Personal Information;

b. Creating a schedule to regularly test and audit that system and train personnel on how to identify potential breaches and the proper procedure following the discovery of a potential breach;

c. Conducting regular secure purges, deletions and destruction of Personal Information that is no longer necessary for its provision of services; and

d. Immediately informing the public of any additional information about the present Data Breach or future data breaches that may occur.

SEVENTH CLAIM FOR RELIEF
INJUNCTIVE RELIEF
(Brought on Behalf of Plaintiff and the Class)

104. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

105. Defendant's wrongful actions and omissions have caused and will continue to cause irreparable harm unless enjoined. Such irreparable harm includes monetary harm, identity theft and fraud, loss of economic and other opportunities, invasion of privacy, embarrassment and harm to reputation. Such irreparable harm will take place, continue, and not cease unless and until enjoined by this Court.

106. The irreparable harm that will be caused Plaintiff and Class members if an injunction does not issue greatly exceeds the inconvenience and expense to Marriott of an appropriate injunction.

107. Accordingly, Plaintiff and Class members are entitled to injunctive relief,

including an order that Defendant immediately take preventative and remedial measures to prevent, stop and remedy the harm, including, *inter alia*: disclosing the full extent and scope of the Data Breach; ceasing its negligent conduct with respect to the Personal Information; implementing measures to stop and prevent exposure of the Personal Information in accord with the best practices of the industry; seeking audit of its security systems by outside security experts; implementing proactive measures to remedy existing misuse of the stolen Personal Information; and establishing a fund from which to reimburse and compensate Plaintiff and Class members for expenses suffered because of the Data Breach or injuries incurred therefrom.

EIGHTH CLAIM FOR RELIEF
VIOLATIONS OF THE CONSUMER PROTECTION ACT
Maryland Code Ann., Com. Law § 13-101, et sec.
(Brought on Behalf of Plaintiff and the Class)

108. Plaintiff realleges and reaffirms the allegations contained in the foregoing paragraphs as though fully set forth herein.

109. By its acts and omissions, Defendant has violated the Maryland Consumer Protection Act ("MCPA"), Md. Code Ann., Com. Law § 13-101, *et sec.*

110. Plaintiff and Class members are consumers and customers within the meaning of the MCPA, and Defendant is a merchant within the meaning of the MCPA.

111. Plaintiff and Class members have standing under the MCPA, which provides, "[a]ny person may bring an action to recover for injury or loss sustained by him as the result of a practice prohibited by this title." Md. Commercial Law Code Ann. § 13-408(a).

112. Defendant failed to maintain reasonable security procedures to protect the Personal Information of Plaintiff and Class members, in violation of Md. Commercial Law Code Ann. §§ 14-3503(a) and 14-3504(a).

113. Defendant deceived and/or misled Plaintiff and Class members with respect to the

security of their Personal Information, and concealed the true vulnerability of personal data entrusted to it and, following the Data Breach, concealed that such data had been accessed by unauthorized third parties, in violation of Md. Commercial Law Code Ann. § 13-301(3).

114. As a direct result of Defendant's violations of the MCPA, Plaintiff and Class members have suffered theft of their Personal Data by unknown hackers and other harm.

115. Accordingly, Plaintiff and Class members are entitled to relief as prayed for hereunder, including all relief available under Md. Commercial Law Code Ann. §§ 14-3508(1) and 13-408(a)-(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for relief and judgment against Defendant, as follows:

a. Certification of the Class as defined herein;

b. Appointment of Plaintiff as Class representative and of her undersigned counsel as Class counsel;

c. An award to Plaintiff and Class members of actual, compensatory, and consequential damages, in an amount exceeding $5,000,000, to be determined by proof;

d. An award to Plaintiff and Class members of statutory damages and penalties

e. An order proving equitable, injunctive and declaratory relief, including the enjoining of Defendant's insufficient data protection practices at issue herein;

f. A declaration that Defendant's acts and practices with respect to the safekeeping of the Personal Information were and are negligent and unlawful;

g. An award to Plaintiff and Class members of their reasonable attorneys fees, litigation expenses and costs of suit incurred through trial and any appeals,

including expert witness fees;

h. An order of restitution and disgorgement;

i. An order that Defendant provide appropriate credit monitoring services to Plaintiff and Class members;

j. An award of pre- and post-judgment interest on any amounts awarded; and

k. Such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Anna L. Haley hereby demands trial by jury of all claims so triable.

Respectfully submitted,

Date: December 12, 2018 By: /s/ Mila F. Bartos

Mila F. Bartos (Bar # 13550)
FINKELSTEIN THOMPSON LLP
3201 New Mexico Avenue, NW
Suite 395
Washington, DC 20016
Telephone: (202) 337-8000
Facsimile: (202) 337-8090 (fax)
mbartos@finkelsteinthompson.com

FINKELSTEIN THOMPSON LLP
Gordon M. Fauth, Jr.
Of Counsel
100 Pine Street, Suite 1250
San Francisco, California 94111
Telephone: (415) 398-8700
Facsimile: (415) 398-8704
gfauth@finkelsteinthompson.com

Attorneys for Individual and Representative Plaintiff Anna L. Haley